OBSAH

1 Úvod **6**

2 Moderní autentizace **7**

3 Kryptografická atributová pověření **9**

3.1 Analýza současného stavu 11

3.2 Problém konstrukce s nízkou výpočetní složitostí 12

3.2.1 Řešení: protokoly založené na algebraickém MACu 12

3.3 Problém efektivní revokace 14

3.3.1 Řešení: kombinace epoch platnosti a omezené randomizace 15

3.4 Problém reálné implementace na embedded zařízeních 17

3.4.1 Řešení: systém Privacy-ABC pro čipové karty 18

4 Další trendy v moderní kryptografii **21**

5 Závěr **21**

Reference **23**

Použité zkratky **33**